(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

10/544172

(43) International Publication Date
26 August 2004 (26.08.2004)

PCT

(10) International Publication Number
WO 2004/073234 A3

(51) International Patent Classification[7]: H04L 9/00

(21) International Application Number:
PCT/US2004/003299

(22) International Filing Date: 5 February 2004 (05.02.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/445,805 7 February 2003 (07.02.2003) US

(71) Applicant *(for all designated States except US)*: **MAGIQ TECHNOLOGIES, INC.** [US/US]; 275 Seventh Avenue, 26th Floor, New York, NY 10001 (US).

(72) Inventors; and

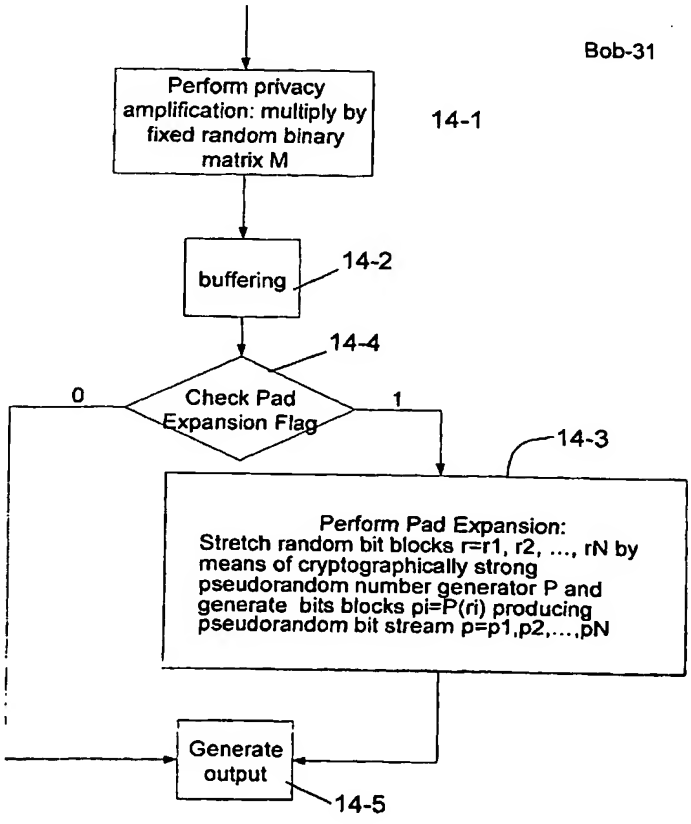
(75) Inventors/Applicants *(for US only)*: **BERZANSKIS, Audrius** [LT/US]; 7 Saint Mary Road, Cambridge, MA 02139 (US). **TRIFONOV, Alexei** [RU/US]; 69 Park Drive, Apt. 8, Boston, MA 02215 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK,

[Continued on next page]

(54) Title: KEY EXPANSION FOR QKD



(57) Abstract: A method of encrypting information using an encryption pad based on keys exchanged between quantum key distribution (QKD) stations is disclosed. The method includes establishing raw keys between two stations using QKD, processing the keys to establish a plurality of matching privacy amplified keys (Fig 8, 14-1) at each station and buffering (14-2) the keys in a shared key schedule. The method also includes the option of expanding (14-4, 14-3) one or more of the keys in the shared key schedule using a stream cipher to create a supply of expanded keys (14-3) that serve as pads for one-time-pad encryption.

WO 2004/073234 A3

TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report*

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

(88) Date of publication of the international search report:
18 November 2004

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US04/03299

A. CLASSIFICATION OF SUBJECT MATTER
IPC(7) : H04L 9/00
US CL : 380/44
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 380/44, 46, 278-

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
Please See Continuation Sheet

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5,768,378 A (TOWNSEND et al.) 16 June 1998 (16.06.1998), abstract, col. 1, lines 52-through col. 2 , line 17, col.2, line 66 through col. 3, line41, col. 4,col. 12, lines 36-67.	1-5.
Y	US 5,757,912 A (BLOW) 26 May 1998 (27.05.1998), the entire document.	1, 3
Y	US 2001/0055389 A1 (HUGHES et al.) 27 December 2001 (27.12.2001), the entire document.	1-5

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search
18 August 2004 (18.08.2004)

Date of mailing of the international search report
09 SEP 2004

Name and mailing address of the ISA/US
Mail Stop PCT, Attn: ISA/US
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
Facsimile No. (703) 305-3230

Authorized officer
Ayaz Sheikh
Telephone No. (703) 305-9648

Form PCT/ISA/210 (second sheet) (January 2004)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US04/03299

Continuation of B. FIELDS SEARCHED Item 3:
West and Proquest. Search Terms: quantum key and one-time-pad, quantum key and authentivation, quantum key and expanded key, quantum key and mater key, key distribution anf quantum key